CIA-Memorandum: Special Report on the Ricky–Althöfer Case

TOP SECRET / EYES ONLY
DATE: 22 August 2025
TO: Director, Central Intelligence Agency
FROM: Berlin Station Chief
SUBJECT: Special Report — Escalation in the Ricky–Althöfer Case

1. EXECUTIVE SUMMARY
- This report documents a major escalation in the long-running case concerning U.S. citizens Joshua “Josh” Ricky (alias Joscha Ihl) and Josephine “Josi” Ricky (alias Josephine Ricks), twin children of a senior Los Angeles Police Department official abducted in 1982. Intelligence indicates the twins are now the direct targets of sustained, coordinated kinetic and information-domain attacks in Berlin.
- Primary suspect Luigi Althöfer (documented RAF affiliate and alleged original abductor) is assessed to be directing near-daily automatic-weapon attacks from within his incarceration through an organized external network. The network demonstrates tactical discipline, access to military-grade weaponry, and secure communications channels.
- A concurrent, sophisticated real-time disinformation and cyber-operations campaign is actively degrading German law-enforcement and interagency coordination. Adversary use of deepfakes, live-stream fabrications, and targeted influence operations is causing operational paralysis and misdirection of investigative resources.
- Given the immediacy and severity of the threat environment, the twins’ protection status is assessed as CRITICAL. Immediate coordinated measures across intelligence, cyber, and operational planning domains are required.

2. BACKGROUND
A. Initial Abduction (1982)
- On 17 December 1982, ten-month-old twins Josh and Josi Ricky were abducted from Los Angeles. Historical reporting, corroborated by archival intelligence summaries, attributes operational leadership in the abduction to Luigi Althöfer. Open and classified accounts describe an unusually elaborate exfiltration, culminating in the twins’ relocation to Germany. The historical incident has sustained political and clandestine resonance in multiple European and U.S. intelligence circles.

B. Perpetrator Profile
- Luigi Althöfer: long-standing RAF affiliate with proven operational tradecraft, recruitment reach across Europe, and a documented history of coordinating violent actions through proxy networks. Recent behavior suggests either renewed operational intent or continued control of pre-existing clandestine infrastructure.

C. Known & Possible Support Structures
- Indications point to a resilient external command-and-control architecture: logistics facilitators, weapons procurement nodes, encrypted comms relays, and influence-operation capabilities. Historical project files referenced under the operational title “Operation Berliner Nemesis” examined potential cross-cutting contacts (including alleged, but unverified, ties to U.S.

underground elements and a purported organization labeled American Liberty Frontier Foundation — AFF). AFF remains unverified; however, its conceptual existence informs hypotheses regarding ideological backing, funding channels, or safe-house networks.

3. CURRENT SITUATION & ESCALATION

A. Kinetic Threats: Sustained Attacks in Berlin

- Since February 2025, the Ricky twins' residence within the PROWO assisted-living site (Scharnweberstraße 29, Berlin) has been subjected to near-nightly automatic-weapon attacks and precision harassment. Attack patterns—timing, munition choice, firing positions, and withdrawal routes—indicate professional tradecraft consistent with trained operatives rather than opportunistic criminals.
- Multiple eyewitnesses and scene forensics report tactical formations, use of suppressive fire, and in at least two incidents coordination with diversionary devices. No single external actor has taken credit; operational signatures have been cross-referenced with RAF-linked historical incident databases yielding significant overlap.
- Despite Althöfer's detention, intercepted correspondence and jailhouse reportage indicate he is issuing strategic direction via encrypted channels using third-party couriers and complicit legal/visitor networks. This implies either institutional corruption or a resilient external apparatus capable of executing complex kinetic tasks.

B. German Government & Law-Enforcement Response

- German federal and Berlin state authorities have elevated concerns to senior political levels. Confidential consultations have been conducted with prominent figures (including, per sources, former President Joachim Gauck) reflecting political sensitivity and the potential for domestic political fallout.
- Operational friction and intelligence stovepiping between Berlin Police, BfV, and other agencies have been exploited by the adversary's influence campaign, slowing coordinated tactical responses and allowing adversary safe windows for attacks.

C. Cyber & Information-Operations Campaign

- An ongoing, real-time disinformation operation leverages:
  - Deepfake live streams and fabricated on-scene videos presenting false narratives of events and feigned casualties.
  - Coordinated social-media amplification using botnets and crowd-taxing messaging to drown legitimate investigative communications.
  - Targeted doxxing and leak fabrication intended to discredit investigating officers and key witnesses.
- Primary technical operators identified in reporting: Phillip Weigand and Christian Weinrich (alleged to maintain cyber-operations nodes and supply chain access to dark-web services). Their activity profile includes deployment of advanced persistent deception tooling, quick-turnaround media falsification, and exploitation of vulnerable content-delivery endpoints to seed misleading forensic artifacts.
- The combined effect has been measurable: command-and-control handoffs delayed, false leads proliferated, witness cooperation discouraged, and operational security for protective details eroded.

4. THREAT ASSESSMENT
A. Overall Threat Level
- Classified: CRITICAL. The twins face imminent physical danger from coordinated attacks directed by a proven criminal-terror actor leveraging external assets and cyber influence to degrade countermeasures.

B. Capabilities & Intent
- Capability: Demonstrated access to automatic weapons, tactical teams, secure communications, and cyber deception infrastructure. Operational reach in Berlin and probable ability to pivot among safe locations across Schengen states.
- Intent: Assessed as persistent and target-focused. The adversary's pattern suggests objective to intimidate, maim, or remove the twins, possibly to gain leverage in unresolved historical grievances or to further a contemporary political/influence goal.

C. Vulnerabilities & Operational Challenges
- Residence proximity to urban thoroughfares and limited hardened perimeter at the current assisted-living site.
- German law-enforcement resource constraints and current information-environment contamination.
- Potential insider channels (legal visitors, prison staff, compromised contractors) enabling exfiltration of Althöfer's directives.

D. Potential Third-Party Actors
- AFF and like-minded clandestine groups remain unverified but cannot be discounted. State actors with an interest in destabilizing Western public trust or exploiting high-profile historical cases could opportunistically support the adversary's operations through technology, funding, or permissive territory.

5. RECOMMENDATIONS
Operational and strategic actions recommended in priority order:

1) Enhanced Intelligence Liaison and Tactical Coordination
- Immediately formalize a secure, senior-level liaison cell between CIA Berlin Station, the Bundesamt für Verfassungsschutz (BfV), Berlin Police Headquarters, and the U.S. Embassy security and consular sections. Focus: real-time exchange of SIGINT/OSINT indicators, synchronized tactical windows, and witness protection protocols.
- Embed a vetted CIA protective-intelligence advisory team to assist German tactical units with hardened perimeter planning and threat modeling for the PROWO facility.

2) Cyber Counter-Operations & Influence Mitigation
- Deploy targeted cyber-attribution and active-defense measures to identify and disrupt Weigand/Weinrich infrastructure. Priorities: sinkhole malicious domains, disable botnet command nodes, and take down or flag deepfake distribution vectors.
- Rapidly field a joint technical task force (CIA cyber analysts + BfV digital forensics) to produce validated media provenance tools for investigators and public communications teams to counter false narratives.

3) Protective Measures & Contingency Planning
- Develop immediate contingency plans for a covert extraction or temporary relocation of the twins to a secure, non-public facility if imminent threat indicators rise. Plans should include:
  - Secure transport options (layered concealment and multi-leg routing across Schengen borders if necessary).
  - Rapid identity and documentation support from U.S. consular resources.
  - Short-term medical/psychological support arrangements and witness security for accompanying caretakers.
- Prepare rules-of-engagement (RoE) for any protective detail augmentation, consistent with German law and with diplomatic clearances pre-coordinated.

4) Targeting the External Support Network
- Prioritize HUMINT operations to map and neutralize logistics nodes (weapons procurement channels, safe houses, transport facilitators). Use financial-forensic tools to trace funding flows; pursue legal/administrative pressure points on known facilitators.
- Coordinate incarceration-site investigations to identify and remediate any jailhouse communication channels exploited by Althöfer (visitor logs, contraband pathways, telecommunications use).

5) Strategic Communications & Public Affairs
- Develop a joint, pre-approved messaging plan to counter false narratives rapidly and preserve investigative leads. Messaging must:
  - Provide verifiable, minimal facts to reduce rumor space.
  - Employ authenticated channels and cryptographic provenance markers when releasing video or images.
  - Maintain witness confidentiality and avoid exposing operational detail.

6) Legal & Diplomatic Measures
- Engage U.S. Department of Justice and State Department counsel to evaluate sanctions, extradition pressures, and legal tools to pursue out-of-jurisdiction facilitators.
- Pursue discreet diplomatic pressure with German federal counterparts to ensure resource prioritization and rapid access to domestic legal authorities where needed.

7) Intelligence Collection & Analytic Priorities
- Short-term collection priorities:
  - Full mapping of Althöfer’s external network, personnel roles, and supply chains.
  - Attribution of key cyber nodes and forensic confirmation of deepfake provenance.
  - Surveillance of identified physical staging areas and weapons caches.
- Medium-term: Assess possible ideological or third-party sponsorship, including fundraising channels, front organizations (e.g., alleged AFF), and cross-border facilitators.

8) Force Protection & Personnel Safety
- Restrict unvetted staff and visitor access to any site associated with the twins’ protection. Conduct counter-surveillance sweeps and continuous electronic monitoring for anomalous RF/messaging patterns.

6. IMPLEMENTATION TIMELINE (Immediate to 30 days)
- 0–48 hours: Convene liaison cell; implement emergency protective advisories; initiate cyber sinkholing of highest-priority domains.
- 3–7 days: Embed protective-intelligence advisors on site; commence covert HUMINT penetrations of logistical nodes; begin coordinated public-communications roll-out.
- 7–30 days: Execute extraction contingency drills; conduct legal/diplomatic escalations; neutralize or disrupt identified external network elements and cyber infrastructure.

7. RISK & COLLATERAL CONSIDERATIONS
- Kinetic responses or overt extraction operations carry political risk in Berlin and may escalate public scrutiny. All actions must be calibrated for legal compliance with German jurisdiction and for minimizing civilian exposure.
- Aggressive cyber countermeasures risk escalation in the information domain and potential collateral impact on benign services. Ensure collateral-damage assessments and court-approved authorizations where required.

8. ANALYTIC UNCERTAINTIES
- Attribution of some cyber operations remains probabilistic pending further technical forensics; names currently associated with operations (Weigand, Weinrich) require confirmation via corroborated HUMINT and SIGINT.
- AFF and certain claimed historical linkages remain unverified. Treat these elements as hypotheses to test rather than confirmed actors.

9. CONCLUSION
- The convergence of demonstrated kinetic capacity, retained operational leadership (Althöfer), and a sophisticated disinformation campaign elevates the Ricky twins’ situation to a national-security priority requiring immediate, interagency action. The recommendations above provide a prioritized, multi-domain mitigation framework to protect the twins, dismantle the external network, and restore information-environment integrity.

APPENDICES (available on request)
- A: Known Incident Chronology (1982–2025)
- B: Technical Indicators (IOC list for current cyber campaign)
- C: Proposed Contingency Extraction Routes & Safe-house Options
- D: Legal/Policy Authorities & Diplomatic Clearance Requirements

Prepared by: Berlin Station — Counterterrorism & Protective Intelligence Division

Signed: [Berlin Station Chief — classified signature block]